

UNITED STATES DISTRICT COURT

for the
Western District of Washington

FILED	LODGED
RECEIVED	
Jul 26, 2021	
CLERK U.S. DISTRICT COURT WESTERN DISTRICT OF WASHINGTON AT TACOMA	
BY	DEPUTY

In the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*
Information Associated with Email Accounts that are
Stored at the Premises Controlled By Google LLC,
More Fully Described in Attachment A

Case No. MJ21-5162

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Email Accounts Controlled by Google LLC, more fully described in Attachment A, incorporated herein by reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 2241(c), 2243	Aggravated Sexual Abuse of a Child Under 12, Sexual Abuse of a Minor
(a)(1); 18 U.S.C. § 2244(a)(5)	Abusive Sexual Contact of a Child Under 12

The application is based on these facts:

- ☒ See Affidavit of FBI Special Agent Kyle McNeal, attached hereto and incorporated herein by reference.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.



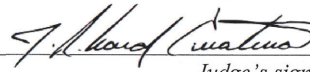
Applicant's signature

KYLE McNEAL, Special Agent, FBI

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 07/26/2021



Judge's signature

City and state: Tacoma, Washington

J. RICHARD CREATURA, U.S. Chief Magistrate Judge

Printed name and title

AFFIDAVIT OF KYLE MCNEAL

STATE OF WASHINGTON)
) SS
COUNTY OF PIERCE)

I, Kyle McNeal, having been duly sworn, state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), assigned to the Special Agent in Charge in Seattle, Washington. I have been an Agent with the FBI since April 2011. My training at the FBI Academy in Quantico, Virginia, included courses in law enforcement techniques, federal criminal statutes, conducting complex criminal investigations, physical and electronic surveillance techniques, and the execution of search warrants. During my employment as a law enforcement officer, I have attended periodic seminars, meetings, and continued training.

2. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to child exploitation and child pornography. I have received training in the area of child pornography and child exploitation. I have also participated in the execution of numerous search warrants involving investigations of child exploitation and/or child pornography offenses. I work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children.

3. I make this affidavit in support of an application for a search warrant for information associated with email accounts:

crankingbullueno@gmail.com

hamingra85@gmail.com

elliotttar@gmail.com

loantee2000@gmail.com

(SUBJECT EMAIL ACCOUNTS) that are stored at premises controlled by Google LLC (hereinafter Google), an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94942. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

4. This also includes any and all information related to preservation record numbers 5263726 and 5946044 (Google LLC) as well as all other subscriber and log records associated with the account. I make this request to search the above accounts for evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2241(c) (Aggravated Sexual Abuse of a Child under 12), 2244(a)(5) (Abusive Sexual Contact of a Child under 12), 2243(a)(1) (Sexual Abuse of a Minor), 3261 (Military Extraterritorial Jurisdiction Act--“MEJA”) and 3238 (MEJA Venue).

5. The facts set forth in this Affidavit are based on the following: my personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of witnesses; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for these search warrants, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are relevant to the determination of probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2241(c)(Aggravated Sexual Abuse of a Child under 12), 2244(a)(5)(Abusive Sexual Contact of a Child under 12), 2243(a)(1)(Sexual Abuse of a

Minor), 3261 (Military Extraterritorial Jurisdiction Act--“MEJA”) and 3238 (MEJA Venue) will be found in the SUBJECT EMAIL ACCOUNTS.

II. SUMMARY OF INVESTIGATION

6. On or about April 5, 2019, the FBI Tacoma Resident Agency was notified from the United States Army Criminal Investigation Division Command (CID) Camp Zama, Japan regarding the sexual abuse of a minor, a 14 year-old girl born on September 12, 2006 (MV1). The abuse occurred on Camp Zama, from 2017 through 2019, when MV1 was there as a military dependent with her family. On January 21, 2021, a Grand Jury indicted TARRUS MAN'DRAL ELLIOTT on four counts of sexual assault of a minor, and a warrant was issued. ELLIOTT is believed to be residing in the Philippines after he fled Japan following the allegations; his whereabouts remain unknown. ELLIOTT is communicating irregularly with his wife, who is working closely with the FBI, using different email addresses.

III. JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. §§ 2711(3)(A)(i); 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense[s] being investigated.” 18 U.S.C. § 2711(3)(A)(i). Federal investigative and charging venue under MEJA lies in 18 U.S.C. § 3238. Where an offender has not been arrested or “brought into any district, an indictment or information may be filed in the district of the last known residence of the offender.” *Id.* Nancy Elliott confirmed with Agents that the last residential address for ELLIOTT and the family in the United States before moving to Japan was 2211 156th St. Ct. E., Tacoma, Washington 98445. This location is located with the Western District of Washington.

IV. PROBABLE CAUSE

8. Camp Zama CID was notified by faculty at John O. Arnn Elementary School, Camp Zama, Japan, that MV1 may have been sexually abused by her father.

1 MV1's teacher, Ms. Lopes, became aware of the incident when associates of MV1
2 informed her of the allegations. Ms. Lopes then reported the information to the school's
3 administration who then passed it on to Camp Zama CID.

4 9. During the investigation, FBI Special Agent Kyle McNeal interviewed
5 Robin Lopes at John O. Arnn Elementary School, Camp Zama, Japan. In the interview,
6 Ms. Lopes provided a poem to SA Kyle McNeal entitled "The Surprise" that MV1 had
7 written:

8 A door opens to a child room, When [sic] it's very dark, a father comes in
9 and wakes the child and takes them downstairs, the whole house is sleeping
10 and so are the family members, the father and the child watch TV until it
11 gets a little late, the father had a surprise for the child and it really did
12 suprise [sic] them, and so then and nothing more the suprise [sic] soon
13 began.

14 10. On April 3, 2019, CID Special Agents interviewed MV1 who confirmed
15 ELLIOTT sexually assaulted her on several occasions. The first instance was
16 approximately a year ago, the last was about two days prior to the interview. MV1
17 disclosed that ELLIOTT would make her perform oral sex upon him and make her touch
18 his genitals. ELLIOTT digitally penetrated MV1 and performed oral sex upon her.
19 Based on the context of the conversation, it is believed that ELLIOTT attempted to
20 penetrate MV1's vagina with his penis. MV1 described this as being painful. According
21 to MV1, these incidents occurred in her home after Mrs. Elliott went to sleep.
22 Additionally, MV1 described being sexually abused at the "Golf Hotel." In a later
23 contact, MV1 positively identified images of the Hotel Golf located in Yamato City,
24 Kanagawa. MV1 further recalled that ELLIOTT abused her, on at least one occasion,
25 while using a device that resembled an electric toothbrush. MV1 was unable to further
26 describe the toothbrush-like object but stated that it was pink in color. ELLIOTT
27 disclosed to MV1 that he had been sexually abused as a child and that he had a sickness.
28 ELLIOTT told her if he did it again, she should tell her mother, Mrs. Elliott.

1 11. On April 3, 2019, CID interviewed ELLIOTT, who provided a video-
2 recorded sworn statement wherein he denied MV1's allegations in their entirety.
3 ELLIOTT did acknowledge that he frequently hugged MV1 and may have, on occasion
4 and unintentionally, grazed her breasts.

5 12. On April 3, 2019, CID collected a sheet and a rug from MV1's room as
6 well as a pink vibrator from Mrs. Elliott's room. While Mrs. Elliott and MV1 showed
7 CID around the house, and when one agent briefly explained DNA to MV1, she
8 spontaneously uttered that CID should collect the rug from the floor in her room.

9 13. On April 3, 2019, Sarah K. Abner conducted a Sexual Assault Forensic
10 Examination. During the exam, MV1 told Abner that "it's happened a lot of places... my
11 room, the last time, sometimes downstairs, my dad's room or hotels... twice in hotels."
12 MV1 further stated, "I don't know if I hurt my dad, but I did try to push him away."
13 When asked if there was anything else about the incident, MV1 remembered "well I spit
14 some stuff on the floor...it wasn't a lot like the time he had stuff come out all over my
15 leg...that was a long time ago though."

16 14. Nurse Abner's examination revealed a mucous type fluid in MV1's vaginal
17 area. Nurse Abner also observed redness with tenderness to the labia minora, posterior
18 fourchette and hymen. These findings are consistent with the ELLIOTT's attempts to
19 vaginally penetrate MV1. MV1 was tested at the Camp Zama Medical Clinic for
20 Sexually Transmitted Diseases (STD's) which came back positive for Chlamydia. MV1
21 denied having sexual contact with anyone other than ELLIOTT.

22 15. On or about February 21, 2020, Mrs. Elliott underwent a Chlamydia
23 trachomatis IgG test. The IgG antibody detection is a marker for a Chlamydia positive
24 immune response, either for current, chronic, or past infections. Based on the results of
25 the test, it suggests that Mrs. Elliott contracted Chlamydia at some point.

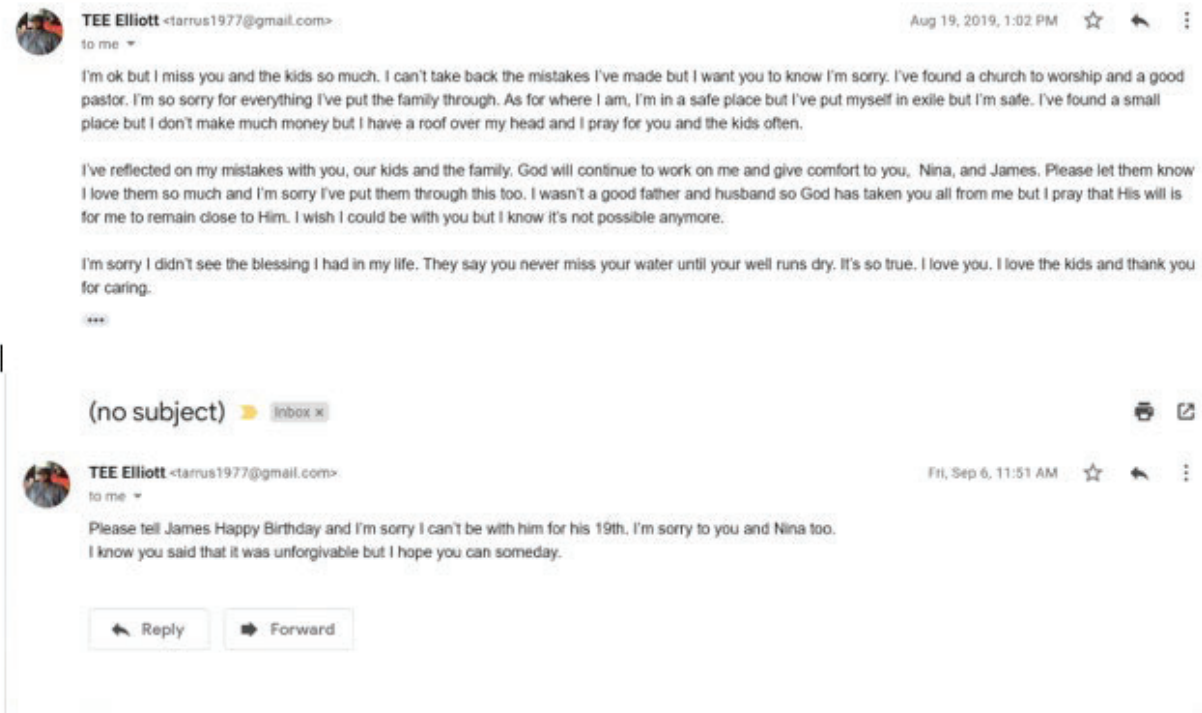
26 16. The FBI Laboratory tested the SANE kit and detected ELLIOTT's DNA on
27 the following swabs: (1) anal/perineal; (2) left breast swab; and (3) right breast swab.
28

1 17. On or about April 13, 2019, ELLIOTT departed Japan through the Narita
2 airport in a failed attempt to visit the Philippines. US Officials successfully convinced
3 Philippine authorities to deny ELLIOTT access to the country after which he returned to
4 Japan.

5 18. On or about April 19, 2019, ELLIOTT was scheduled to depart Japan for
6 Hawaii. The Hawaiian USAO was prepared to interdict ELLIOTT upon his arrival and
7 execute a search warrant for his digital devices. Instead, ELLIOTT sent a message to
8 Nancy Elliott claiming that an accident on the train had forced him to miss his flight.
9 ELLIOTT apologized and told Nancy Elliott that he would attempt to get on the flight the
10 following day. Instead of traveling to Hawaii as planned, financial records indicated that
11 ELLIOTT purchased a flight on Air Asia (KH) for \$251.66 in addition to a \$3.00 Inflight
12 Internet Service fee. ELLIOTT told Nancy Elliott that he was in Korea, but (KH) is the
13 abbreviation for Cambodia.

14 19. ELLIOTT's current whereabouts are unknown although he has had email
15 communications with Nancy Elliott. Nancy Elliott provided consent for SA McNeal to
16 monitor her email communications with ELLIOTT. The following communications took
17 place between ELLIOTT and Nancy Elliott.

18 **Email from TARRUS1977@GMAIL.COM**



Email from TARRUS1977@HOTMAIL.COM

----- Forwarded message -----
 From: te <tarrus1977@hotmail.com>
 Date: Wed, Nov 27, 2019 at 09:02
 Subject: I'm sorry
 To: Nancy Elliott <nelliott@gmail.com>

To whom it may concern, this will be my final to you. Everything I've done I'm sorry. I will take my life tonight and I know it will disappoint some of you and others will feel relieved. Goodbye

20. On November 27, 2019, SA McNeal received the email noted above from Nancy Elliott. Emergency Disclosure requests were sent to Google for records pertaining to the whereabouts of ELLIOTT. Based on the IP address provided by Google on or about November 27, 2019, it appeared that ELLIOTT was in the Philippines.

21. Nancy Elliott has confirmed that both Tarrus1977@gmail.com and Tarrus1977@hotmail.com belong to ELLIOTT. Both prior to and since the allegations as demonstrated by the identified messages, Nancy Elliott has received numerous messages from the SUBJECT ACCOUNTS that she believes to have come from ELLIOTT.

22. On May 1, 2020, ELLIOTT appeared to contact Nancy Elliott through email account elliotttar@gmail.com. The email is displayed below.

----- Forwarded message -----
From: **tar elliott** <elliotttar@gmail.com>
Date: Fri, May 1, 2020 at 18:38
Subject: ok
To: <[n\[REDACTED\]@gmail.com](mailto:n[REDACTED]@gmail.com)>

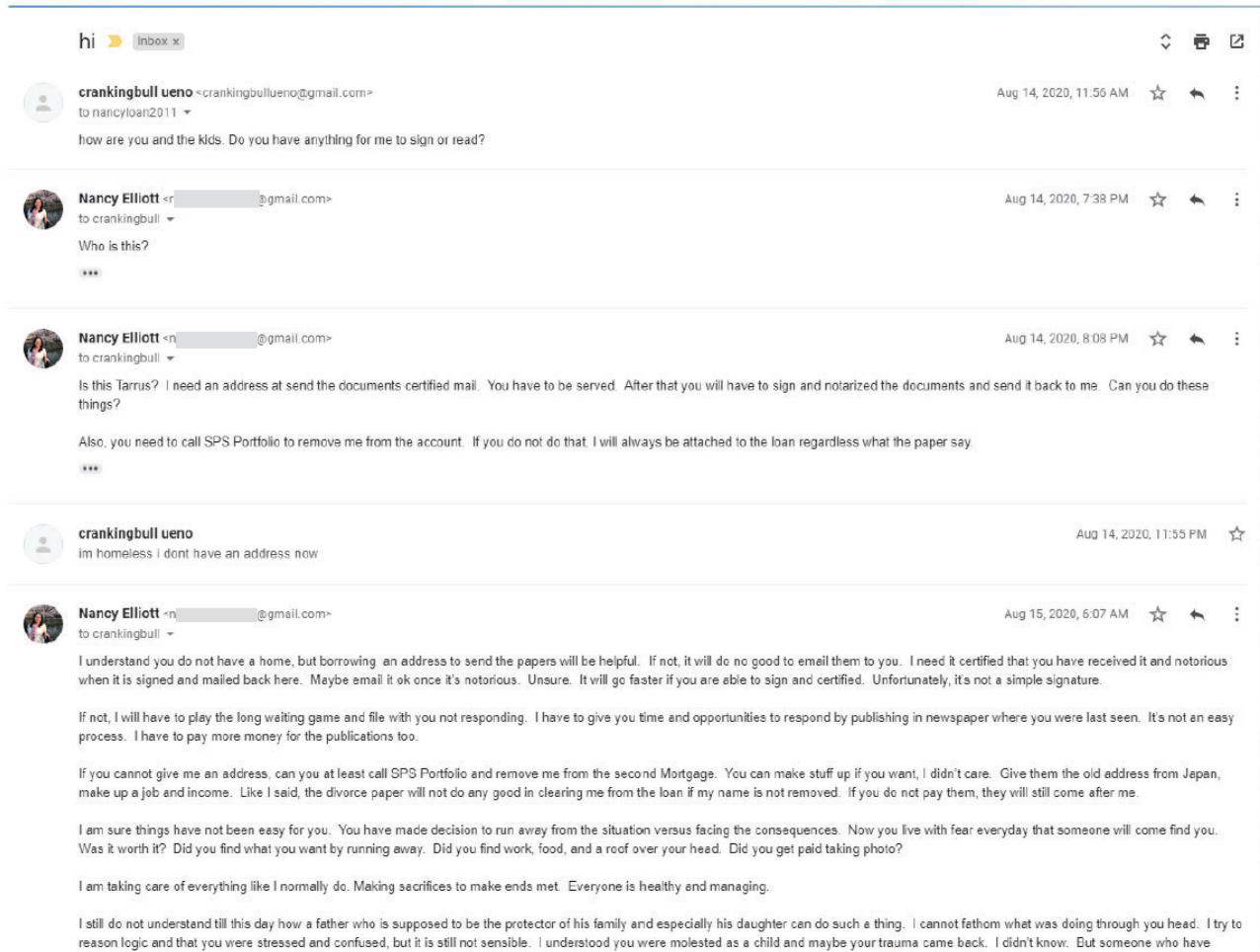
my phone so i lost my account information. are you amd the kids alright?

23. On August 14, 2020, ELLIOTT appeared to contact Nancy Elliott through email account crankingbullueno@gmail.com. An excerpt from the email conversation is displayed below.

//

//

//



24. On January 20, 2021, ELLIOTT appeared to contact Nancy Elliott through email account hamingra85@gmail.com. The email is displayed below.

----- Forwarded message -----

From: **Ingra Ham** <hamingra85@gmail.com>

Date: Wed, Jan 20, 2021 at 09:58

Subject: They canceled my passports

To: <[n\[REDACTED\]@gmail.com](mailto:n[REDACTED]@gmail.com)>

Hello it's mean I'm sorry i havent been able to contact the mortgage company. I understand what position I left you in. I'm on the run and things aren't easy for me. The government canceled my passports so I can't travel so I'm stuck here. I won't kill myself so the only thing I can do is move on. This will be the last email I'll send to you I'm sorry I love you and the kids although my actions didn't show that. Please take care and forgive me what all I lve done.

Forever sorry

Me

25. On January 24, 2021, ELLIOTT appeared to contact Nancy Elliott through email account loantee2000@gmail.com. The email is displayed below.

----- Forwarded message -----

From: **Ingra Ham** <loantee2000@gmail.com>

Date: Sun, Jan 24, 2021 at 08:46

Subject: Can't say

To: [n\[REDACTED\]@gmail.com](mailto:n[REDACTED]@gmail.com) <[n\[REDACTED\]@gmail.com](mailto:n[REDACTED]@gmail.com)>

I can't say where I am but I'm safe with a place to sleep and food not a lot but I'm eating. I'm truly sorry for everything.

26. At all relevant times, Nancy Elliott was a Department of Defense civilian employee residing overseas. As such, ELLIOTT was a dependent of Nancy Elliott and accompanying the Armed Forces overseas. ELLIOTT's alleged offenses against MV1 are subject to prosecution in federal district court for crimes committed outside the United States as if the offenses were committed within the special maritime and territorial jurisdiction of the United States. *See* MEJA, 18 U.S.C. §§ 3261-3267.

V. SUBJECT'S USE OF ELECTRONIC COMMUNICATION SERVICES

27. In my training and experience, and based upon the training and experience of other FBI special agents with whom I have consulted, I have learned that Google ("Providers") make a variety of online services available, including electronic mail

1 (“email”) access, to the general public. These Providers manage email accounts at the
2 domain names “gmail.com” like the SUBJECT EMAIL ACCOUNTS. Subscribers
3 obtain an account by registering with the Providers. During the registration process, the
4 Providers asked subscribers to provide basic personal information. Therefore, the
5 Providers’ computers are likely to contain stored electronic communications (including
6 retrieved and unretrieved email for the Providers’ subscribers) and information
7 concerning subscribers and their use of the Providers’ services, such as account access
8 information, email transaction information, and account application information. In my
9 training and experience, such information may constitute evidence of the crimes under
10 investigation because the information can be used to identify the account’s user or users.

11 28. In general, an email message that is sent to the Providers’ subscriber is
12 stored in the subscriber’s “mail box” on the Providers’ servers until the subscriber deletes
13 the message. If the subscriber does not delete the message, the message can remain on
14 the Providers’ servers indefinitely. Even if the subscriber deletes the message, it may
15 continue to be available on the Providers’ servers for a certain period of time.

16 29. When the subscriber sends an email message, it is initiated at the user’s
17 computer, transferred via the Internet to the Providers’ servers, and then transmitted to its
18 end destination. The Providers often save a copy of the email message sent. Unless the
19 sender of the message specifically deletes the message from the Providers’ server, the
20 message can remain on the system indefinitely. Even if the sender deletes the email
21 message, it may continue to be available on the Providers’ servers for a certain period of
22 time.

23 30. A sent or received email message typically includes the content of the
24 message, source and destination addresses, the date and time at which the message was
25 sent, and the size and length of the email message. If an email user writes a draft
26 message but does not send it, that message may also be saved by the Providers but may
27 not include all of these categories of data.
28

1 31. A Providers' subscriber can also store files, including email messages,
2 address books, contact or buddy lists, calendar data, photographs, and other files, on
3 servers maintained and/or owned by the Providers. In my training and experience,
4 evidence of who was using an email account may be found in address books, contact or
5 buddy lists, email messages in the account, attachments to email messages, including
6 photographs and files, and photographs and files stored in relation to the account.

7 32. Subscribers to the Providers might not store on their home computers or
8 other digital devices copies of the email messages stored in their Providers account. This
9 is particularly true when they access their Providers' account through via the internet, or
10 if they do not wish to maintain particular email messages or files in their residence.

11 33. In general, the Providers ask each of their subscribers to supply certain
12 personal identifying information when registering for an email account. This information
13 can include the subscriber's full name, physical address, telephone numbers and other
14 identifiers, alternative email addresses, and, for paying subscribers, means and source of
15 payment (including any credit or bank account number). In my training and experience,
16 such information may constitute evidence of the crimes under investigation because the
17 information can be used to identify the account's user or users.

18 34. These email Providers typically retain certain transactional information
19 about the creation and use of each account on their systems. This information can
20 include the date on which the account was created, the length of service, records of log in
21 (i.e., session) times and durations, the types of service utilized, the status of the account
22 (including whether the account is inactive or closed), the methods used to connect to the
23 account (such as logging into the account via the Providers' website), and other log files
24 that reflect usage of the account. In addition, these email Providers often have records of
25 the IP address used to register the account and the IP addresses associated with particular
26 logins to the account. Because every device that connects to the Internet must use an IP
27 address, IP address information can help to identify which computers or other devices
28 were used to access the SUBJECT EMAIL ACCOUNTS.

35. In some cases, email account users will communicate directly with the Providers about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. The Providers typically retain records about such communications, including records of contacts between the user and the Providers' support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

36. I know that Google offers approximately 15 GB of free storage space per email address. This allows users to store a large amount of emails and other related content. Google Drive (formerly known as Google Docs) is a free online "cloud" storage that allows users to share files from any device. With Google Drive, a user can share files in lieu of sending email attachments. Picasa is a photo-sharing website owned by Google that allows users to post and share images with other individuals. Google also offers other distinct services, including video chat and Google+ Photos. All of these services are very useful tools that the user of the Google account could be using to store and share images of child pornography. Google also allows its users, through its mobile services, to access their email account(s), stored images, and other content at any time from any computer with Internet access.

VI. PAST EFFORTS TO OBTAIN EVIDENCE

37. I understand that the contents of the SUBJECT EMAIL ACCOUNTS can only be obtained in the Ninth Circuit, by means of a search warrant issued under authority of 18 U.S.C. § 2703(a), 2703(b)(1)(A), 2703(c)(1)(A), and Federal Rule of Criminal Procedure 41(e)(2)(b).

38. To my knowledge, there have been no other prior attempts to secure a search warrant to search and seize these records. In January 2021 and May 2021, preservation letters were sent to Google respectively requesting that the contents of the

1 SUBJECT EMAIL ACCOUNTS be preserved, pursuant to 18 U.S.C. § 2703(f)(1), for a
2 period of 90 days.

3 **VII. GENUINE RISKS OF DESTRUCTION OF EVIDENCE**

4 39. Based on my experience and training, it is not uncommon for technically
5 sophisticated criminals to use encryption or programs to destroy data that can be
6 triggered remotely or by a pre-programed event to keystroke, or other sophisticated
7 techniques to hide data. In this case, the data sought is stored on a server belonging to the
8 Providers. If that data is accessed and deleted by the user, by either deleting the emails or
9 any associated contact lists, the content would not be retrievable. Unlike traditional
10 computer forensics where a hard drive can be searched and deleted documents recovered,
11 information stored in an enterprise storage system is irretrievable once it has been
12 deleted.

13 **VIII. PROTOCOL FOR SORTING SEIZABLE ELECTRONICALLY**
14 **STORED INFORMATION**

15 40. In order to ensure that agents are limited in their search only to the contents
16 of the SUBJECT EMAIL ACCOUNTS and any attachments, stored instant messages,
17 stored voice messages, documents, and photographs associated therewith; in order to
18 protect the privacy interests of other third parties who have accounts with the Providers;
19 and in order to minimize disruptions to normal business operations of Google; this
20 application seeks authorization to permit agents and employees of Google to assist in the
21 execution of the warrant, pursuant to 18 U.S.C. § 2703(g), as follows:

22 a. The search warrants will be presented to Google with direction that
23 it identifies and isolates the SUBJECT EMAIL ACCOUNTS and associated records
24 described in Section I of Attachment B.

25 b. Google will also be directed to create an exact duplicate in electronic
26 form of the SUBJECT EMAIL ACCOUNTS and associated records specified in Section I
27 of Attachment B, including an exact duplicate of the content of all email messages stored
28 in the SUBJECT EMAIL ACCOUNTS.

1 c. Google shall then provide an exact digital copy of the contents of the
2 SUBJECT EMAIL ACCOUNTS, as well as all other records associated with the account,
3 to me, or to any other agent of the FBI. Once the digital copies have been received from
4 Google, the copies will, in turn, be forensically imaged and only those images will be
5 reviewed and analyzed to identify communications and other data subject to seizure
6 pursuant to Section II of Attachment B. The original digital copies will be sealed and
7 maintained to establish authenticity, if necessary.

8 d. I, and or other agents of the FBI, will thereafter review the forensic
9 images, and identify from among that content those items that come within the items
10 identified in Section II to Attachment B, for seizure. I, and/or other agents of the FBI,
11 will then copy those items identified for seizure to separate media for future use in
12 investigation and prosecution. The forensic copies of the complete content of the
13 SUBJECT EMAIL ACCOUNTS will also then be sealed and retained by the FBI, and
14 will not be unsealed absent Court authorization, except for the purpose of duplication of
15 the entire image in order to provide it, as discovery, to a charged defendant.

16 41. Analyzing the data contained in the forensic image may require special
17 technical skills, equipment, and software. It could also be very time-consuming.
18 Searching by keywords, for example, can yield thousands of “hits,” each of which must
19 then be reviewed in context by the examiner to determine whether the data is within the
20 scope of the warrant. Merely finding a relevant “hit” does not end the review process.
21 Keywords used originally need to be modified continuously, based on interim results.
22 Certain file formats, moreover, do not lend themselves to keyword searches, as keywords
23 search text, and many common electronic mail, database, and spreadsheet applications
24 (which may be attached to email) do not store data as searchable text. The data is saved,
25 instead, in proprietary non-text format. And, as the volume of storage allotted by service
26 providers increases, the time it takes to properly analyze recovered data increases as well.
27 Consistent with the foregoing, searching the recovered data for the information subject to
28

1 seizure pursuant to this warrant may require a range of data analysis techniques and may
2 take weeks or even months.

3 42. Based upon my experience and training, and the experience and training of
4 other agents with whom I have communicated, it is necessary to seize all emails, chat
5 logs and documents, that identify any users of the SUBJECT EMAIL ACCOUNTS and
6 any emails sent or received in temporal proximity to incriminating emails that provide
7 context to the incriminating communications.

8 43. All forensic analysis of the image data will employ only those search
9 protocols and methodologies reasonably designed to identify and seize the items
10 identified in Section II of Attachment B to the warrant.

11 **IX. FACTUAL BASIS FOR SEALING AND NON-DISCLOSURE**


12 44. The government requests, pursuant to the preclusion of notice provisions of
13 Title 18, United States Code, Section 2705(b), that Google be ordered not to notify any
14 person (including the subscriber or customer to which the materials relate) of the
15 existence of this warrant for such period as the Court deems appropriate. The
16 government submits that such an order is justified because notification of the existence of
17 this Order would seriously jeopardize the ongoing investigation. ELLIOTT's current
18 whereabouts are unknown and he poses a threat to the community. The FBI is currently
19 attempting to locate him pursuant to an active warrant. Premature notification of this
20 investigation could cause further flight from prosecution, risk destruction of or tampering
21 of evidence or otherwise seriously jeopardize this investigation. *See* 18 U.S.C. § 2705(b).
22 Such a disclosure would give the subscriber an opportunity to destroy evidence, change
23 patterns of behavior, notify confederates, or flee.

24 45. It is further respectfully requested that this Court issue an order sealing, until
25 further order of the Court, all papers submitted in support of this application, including the
26 application and search warrant until the earliest of the following: (a) two weeks following
27 the unsealing of any charging document in a matter for which the warrant was issued; (b)
28

1 two weeks following the closure of the investigation for which the warrant was issued; or
 2 (c) sixteen months following issuance of the warrant, unless the Court, upon motion of the
 3 government for good cause, orders an extension of this Order. I believe that sealing this
 4 document is necessary because the items and information to be seized are relevant to an
 5 ongoing investigation.

6 X. CONCLUSION

7 46. Based on the forgoing, I request that the Court issue the proposed search
 8 warrant. Pursuant to 18 U.S.C. § 2703(g), the government will execute this warrant by
 9 serving the warrant on Google. Because the warrant will be served on Google, who will
 10 then compile the requested records and data, reasonable cause exists to permit the
 11 execution of the requested warrant at any time in the day or night. Accordingly, by this
 12 Affidavit and Warrant, I seek authority for the government to search all of the items
 13 specified in Section I, Attachment B (attached hereto and incorporated by reference
 14 herein) to the Warrant, and specifically to seize all of the data, documents and records
 15 that are identified in Section II to that same Attachment.

16
 17 
 18 _____
 19 KYLE MCNEAL, Affiant
 20 Special Agent
 Federal Bureau of Investigation

21 Subscribed and sworn to me by telephone on July 26, 2021.

22
 23 
 24 _____
 25 J. RICHARD CREATURA
 26 United States Chief Magistrate Judge
 27
 28

ATTACHMENT A
Place to Be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including location history data, sourced from methods including GPS, Wi-Fi, and Bluetooth, and all preserved data associated with:

- 1. crankingbullueno@gmail.com;**
- 2. hamingra85@gmail.com;**
- 3. elliotttar@gmail.com; and**
- 4. loantee2000@gmail.com.**

as well as all location history data and other subscriber and log records associated with the SUBJECT ACCOUNTS, to include the IIS (Internet Information Services) logs associated with any associated Google Drive accounts, which are located at premises owned, maintained, controlled or operated by Google LLC, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

**ATTACHMENT B
ITEMS TO BE SEIZED**

I. Items to be to be Provided for Search

All electronically stored information and communications contained in, related to, and associated with, including all preserved data associated with, the following
SUBJECT ACCOUNTS:

1. **crankingbullueno@gmail.com;**
2. **hamingra85@gmail.com;**
3. **elliotttar@gmail.com; and**
4. **loantee2000@gmail.com.**

including any and all information related to preservation record numbers 5263726 and 5946044 (Google LLC) as well as all subscriber records associated with the SUBJECT ACCOUNTS, including (1) name; (2) address; (3) records of session times; (4) length of service (including start date) and types of services utilized; (5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address; (6) account log files (login IP address, account activation IP address, and IP address history); (7) detailed billing records/logs; (8) means and source of payment; (9) lists of all related accounts; (10) all email content; (11) all other account information; (12) all other profile information; (13) all contact lists; (14) all calendar content; and (15) any and all records of communications between Google, and any other person about issues relating to the SUBJECT ACCOUNT, such as technical problems, billing inquiries, or complaints from other users about the specified account. This is to include records of contacts between the subscribers and the providers' support services, as well as records of any actions taken by the provider or subscriber as a result of the communications. All electronically stored information location history data, sourced from methods including GPS, Wi-Fi and Bluetooth. All items shall be provided in Universal Time Coordinated (UTC) and disclosed to the government within fourteen (14) days of service of this warrant.

1 **II. Items to be Seized**

2 From all electronically stored information and communications contained in,
 3 related to, and associated with, including all preserved data associated with, the
 4 SUBJECT EMAIL ACCOUNTS listed in Attachment A, all information described below
 5 that constitutes fruits, evidence, and instrumentalities of the crimes of 18 U.S.C. §§
 6 2241(c)(Aggravated Sexual Abuse of a Child under 12), 2244(a)(5)(Abusive Sexual
 7 Contact of a Child under 12), 2243(a)(1)(Sexual Abuse of a Minor), 3261 (Military
 8 Extraterritorial Jurisdiction Act--“MEJA”) and 3238 (MEJA Venue), including any and
 9 all of the following records:

- 10 (a) Message header data required to trace any user associated with the
 11 account and its access;
- 12 (b) Subscriber details provided by the user when creating the account;
- 13 (c) IP log-on data for access to the accounts;
- 14 (d) Subscriber information, including names, addresses, dates of birth, contact
 15 details and any other personal information supplied by the subscriber such
 16 as the means and source of payment for any service;
- 17 (e) User connection information, including session times and durations and IP
 18 addresses assigned during the relevant period;
- 19 (f) All contact lists, address lists, buddy lists or other such data associated with
 20 the account;
- 21 (h) All opened or unopened communications in the SUBJECT ACCOUNTS
 22 between April 5, 2019 through July 13, 2021;
- 23 (i) All photographs and images found in the account, including IP data and any
 24 other traceable details of any users who have accessed or downloaded the
 25 photographs and images; and
- 26 (j) All location history data, sourced from methods including GPS, Wi-Fi, and
 27 Bluetooth between April 5, 2019 through July 13, 2021.
- 28